

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
EMAIL ACCOUNTS THAT ARE STORED
AT PREMISES CONTROLLED BY
GOOGLE AND YAHOO

Magistrate Nos. 16-700M
16-702M
[UNDER SEAL]

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Brian Stevens, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with certain accounts that are stored at premises controlled by Google, an email provider headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043 and certain accounts that are stored at a premises controlled by Yahoo, an email provider headquartered at 701 First Avenue, Sunnyvale, CA 94089. The information to be searched is described in the following paragraphs and in Attachment A (Google) and Attachment B (Yahoo). This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google and Yahoo to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment C. Upon receipt of the information described in Section I of Attachment C, government-authorized persons will review that information to locate the items described in Section II of Attachment C.

2. I am an investigative or law enforcement officer of the United States within the meaning of Title 18, United States Code, Section 2510(7); that is, an officer of the United States

who is empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in Title 18, United States Code, Section 2516.

3. I have been a Special Agent with the Federal Bureau of Investigation (FBI) since January, 2015. During that time, I have received training in computer crime investigations. I have also received training and gained experience in interviewing and interrogation techniques, the execution of federal search and seizure warrants, and the identification and collection of computer-related evidence. I am currently assigned to the Pittsburgh Division Cyber Intrusion Squad.

4. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Sections 371 (Conspiracy), 1030(a)(2) (Obtaining Information through an Unauthorized Access of a Protected Computer), 1030(a)(4) (Unauthorized Access of a Protected Computer in Furtherance of Fraud), and 1030(a)(5) (Intentional Damage to a Protected Computer), 1343 (Wire Fraud), 1344 (Bank Fraud), 1349 (Conspiracy to Commit Wire/Bank Fraud) and 1956 (Laundering of Monetary Instruments), (hereinafter the "Target Offenses") have been committed by as yet unknown persons in control of an email account described below. There is also probable cause to search the accounts described in Attachment A (Google) and Attachment B (Yahoo) for evidence, instrumentalities, contraband or fruits of these crimes further described in Attachment C.

JURISDICTION

6. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) &

(c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

EXPLANATION OF RELEVANT TERMS AND CONCEPTS

7. “Server” is a centralized computer that provides services for other computers connected to it through a network or Internet. The computers that use the server’s services are sometimes called “clients.” When a user accesses email, Internet web pages, or accesses files stored on the network itself, those files are pulled electronically from the server, where they are stored, and are sent to the client’s computer via the network or Internet. Notably, server computers can be physically located in any location; for example, it is not uncommon for a network’s server to be located hundreds (or even thousands) of miles away from the client computers. In larger networks, it is common for servers to be dedicated to a single task. For example, a server that is configured so that its sole task is to support a World Wide Web site is known simply as a “Web server.” Similarly, a server that only stores and processes e-mail is known as a “mail server.”

8. “Internet Protocol address” or “IP address” is a unique numeric address used to identify computers on the Internet. The standard format for IP addressing consists of four numbers between 0 and 255 separated by dots, e.g., 149.101.10.40. Every computer connected to the Internet (or group of computers using the same account to access the Internet) must be assigned an IP address so that Internet traffic, sent from and directed to that computer, is directed properly from its source to its destination. Internet Service Providers (ISPs) assign IP addresses to their customers’ computers.

9. A “bot” is a computer that has been compromised by malicious software for use in completing malicious and/or illegal tasks via remote direction. Most users that have a computer acting as a bot are not aware that their computers have been compromised.

10. A “botnet” is a collection of Internet-connected computers (often referred to as zombie computers) whose security defenses have been breached and control ceded to a malicious party. Each such compromised device, or bot, is created when a computer is penetrated by malware. Typically, the malware directs the computer to “call back” or connect to command and control (c2) servers which are controlled by hackers. These servers can be used to control the various bots. Furthermore, the malware installed on a victim’s computer often blocks access to more than 100 popular anti-virus and security programs so that the infected user cannot download the software to fight the malware.

11. A “domain name” is a unique name, corresponding to one or more numeric IP addresses, used to identify a particular web page or set of web pages on the internet.

12. “Domain Name System” (DNS) is the way that Internet domain names are located and translated into IP addresses. When a Web address (URL) is typed into a browser, DNS servers return the IP address of the Web server associated with that name.

13. “Bullet Proof (bp) Hosting” is a service provided by some domain hosting or web hosting firms that allows their customer considerable leniency in the kinds of material they may upload and distribute. Often, a bulletproof host allows a content provider to bypass the laws or contractual terms of service regulating Internet content and service use in its own country of operation, as many of these “bulletproof hosts” are often located in different countries than the perpetrators. This allows a criminal hacker to use servers provided with bullet proof protections in place to hide their identity from law enforcement.

14. “Malware,” short for malicious software, is any software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems. Malware is defined by its malicious intent, acting against the requirements of the computer user, and does not include software that causes unintentional harm due to some deficiency.

15. “Money mules” are people who are used to transport and launder stolen money or some kind of merchandise. Cyber-criminals often recruit money mules to use stolen credit card information or launder proceeds from malware victims.

16. “Ransomware” is a type of malware that prevents or limits users from accessing their system. This type of malware forces its victims to pay the ransom through certain online payment methods in order to grant access to their systems, or to get their data back. Some ransomware encrypts files (called Cryptolocker) so that they cannot be read without a key to decrypt the files.

GOOGLE AND YAHOO EMAIL AND RELATED SERVICES

17. This affidavit is made in support of an application for search warrants pertaining to certain email accounts and related Google services provided by the web-based electronic mail and remote computing service provider known as Google. Additionally, this affidavit is made in support of an application for a search warrant pertaining to a certain email account and related Yahoo services provided by the web-based electronic mail and remote computing service provider known as Yahoo. The accounts (hereinafter sometimes collectively referred to as the “Target Accounts”) to be searched are:

Google: krasi2222@gmail.com
Yahoo: autodali69@yahoo.com

18. Target Accounts are Google and Yahoo email accounts. In my training and experience, I have learned that Google and Yahoo provide a variety of online services, including

electronic mail access, to the public. Google allows subscribers to obtain email accounts at the domain name gmail.com like the email accounts listed in Attachment A. Yahoo allows subscribers to obtain email accounts at the domain name yahoo.com like the email accounts listed in Attachment B. Subscribers obtain an account by registering with Google or Yahoo (Provider). During the registration process, Provider asks subscribers to provide basic personal information. Therefore, the computers of Google and Yahoo are likely to contain stored electronic communications (including retrieved and unretrieved email for Google or Yahoo subscribers) and information concerning subscribers and their use of services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. In general, I know that an email that is sent to a Google or Yahoo subscriber is stored in the subscriber's "mail box" on Provider's servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on Provider's servers indefinitely. Even if the subscriber deletes the email, it may continue to be available on Provider's servers for a certain period of time.

19. A Google or Yahoo subscriber can also store with the provider files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by Providers. In addition, subscribers to these accounts may enlist other internet services that are associated with the account. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, attachments to emails, including pictures and files.

20. In addition, Google subscribers may activate other Google services which will be linked to the account, such as AdMob, Android, Blogger, Gmail, Google Ad Planner, Google AdSense, Google Adwords, Google Alerts, Google Analytics, Google Calendar, Google Chrome Sync, Google Drive, Google Play, Google Play Music, Google Sites, Google Talk, Google URL Shortener, Google Wallet, Google Webmaster Tools, Google+, Has Google Profile, Has Plusone, Location History, Merchant Center, Picasa Web Albums, Web History, and YouTube.

INVESTIGATIVE RELEVANCE OF EMAIL ACCOUNT SERVICES

21. In my training and experience, subscriber information collected by service providers may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location or illicit activities.

22. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the IP address used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account. Common IP

addresses between accounts can also help to identify other accounts which are controlled by the same user and thus help to identify the user.

23. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In addition, email providers can store information relating to the location of a user, as well as information linking accounts to the same user, such as cookies and registration/secondary email accounts. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

24. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, email providers typically log the IP addresses from which users access the

email account along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculcate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

25. As a federal agent, I am trained and experienced in identifying communications relevant to the crimes under investigation. The personnel of Google and Yahoo (i.e., the "Providers") may not be. I also know that the manner in which the data is preserved and analyzed may be critical to the successful prosecution of any case based upon this evidence. Computer Forensic Examiners are trained to handle digital evidence. Google and Yahoo employees may not be. It would be inappropriate and impractical, however, for federal agents to search the vast computer networks of Google and Yahoo for the relevant accounts and then to analyze the contents of those accounts on the premises of Google and Yahoo. The impact on Google's and Yahoo's business would be severe.

26. In order to accomplish the objective of the search warrant with a minimum of interference with the business activities of Google and Yahoo, to protect the rights of the subjects of the investigation and to effectively pursue this investigation, authority is sought to allow

Google and Yahoo to make a digital copy of the entire contents of the information subject to search specified in Attachment A (Google) and Attachment B (Yahoo). That copy will be provided to me or to any authorized federal agent. The contents will then be analyzed to identify records and information subject to seizure pursuant to Attachment C.

27. Executing a warrant to search Google and Yahoo email accounts requires an approach similar to the standard approach for executing a warrant to search papers stored in a file cabinet. Searching the subject email account in this case for evidence of the target crimes will require that agents cursorily inspect all emails produced by Google and Yahoo in order to ascertain which contain evidence of those crimes, just as it is necessary for agents executing a warrant to search a filing cabinet to conduct a preliminary inspection of its entire contents in order to determine the documents which fall within the scope of the warrant. In addition, keyword searches alone are inadequate to ensure that law enforcement can discover all information subject to seizure pursuant to Attachment C. Keywords search text, but many common electronic mail, database and spreadsheet applications files (which files may have been attached to electronic mail) do not store data as searchable text.

DETAILS OF PROBABLE CAUSE

28. Approximately a year ago, the FBI joined German and other international law enforcement partners investigating a sophisticated cyber-criminal infrastructure called "Avalanche." Avalanche is a hosting infrastructure that is composed of a worldwide network of servers that is controlled via a highly organized central control system. The Avalanche operators rent out access to the network to other cyber criminals interested in acquiring bulletproof hosting services over which the criminals conduct malware attacks and operate money mule campaigns to launder the illegal proceeds. In fact, your affiant has personally observed postings on

exclusive underground online criminal forums in which the unidentified Avalanche suspects wrote postings offering these services to other cyber criminals.

29. Avalanche is remarkable for both the volume and variation of malware and money mule operations funneled through its servers. Avalanche has also proven to be extremely resilient to counter measures because of the frequency with which the servers in its infrastructure are changed. Moreover, information obtained via federal grand jury subpoena revealed that the servers used in Avalanche are often paid for through stolen credit cards or by other means designed to thwart detection by law enforcement.

30. Avalanche operates through a layered, or tiered, network of servers that are controlled through a carefully maintained back-end infrastructure. Your affiant queried open source public databases and learned that, at the lowest level of the infrastructure, the administrators of Avalanche register domain names with a handful of registrars on behalf of other cyber criminals. These domains serve as the infection point to distribute various types of malware, or to operate money mule campaigns. Victim machines connect to these domains through different mechanisms, such as when a vulnerable web browser or webpage is exploited and causes the victim machine to connect to the malicious domain. The perpetrators configure these domain names and associated DNS servers in such a way that causes the IP addresses for the domains to change frequently (also known as “fluxing”). The purpose of this fluxing is to thwart detection of malicious domains and IP addresses by law enforcement.

31. For example, once a machine is infected with malware, the machine is instructed to contact a domain that points to a “first-level” server within the Avalanche infrastructure. This first-level usually consists of between 20 and 30 active servers that receive communications directly from infected victim machines that are instructed by the malware to “call back” to the

first-level and await further commands. In the Avalanche infrastructure, first-level servers are used, on average, for less than 30 days in order to thwart detection by law enforcement. Because first-level servers are changed with such frequency, they are extremely difficult to monitor or search before the perpetrators dispose of them and utilize new servers.

32. The first-level Avalanche servers forward information (such as stolen login or account credentials) from victim machines to “second-level” servers in the Avalanche infrastructure that organize the information and forward it to “back-end” control servers. On July 16, 2015, the FBI began to monitor traffic on a number of U.S.-based “second-level” servers pursuant to pen register/trap and trace devices authorized by order of this Court. The data from these pen registers has enabled the FBI, in conjunction with its foreign law enforcement partners, to “map out” the Avalanche infrastructure.

33. Beginning in early 2016, a pernicious new type of malware, GozNym, began to run over Avalanche and infected many U.S. victims. A Title III wiretap on the Avalanche domain registration server, which was located in the United States until approximately June 2016, revealed that the server was querying many domains that security researchers had identified as hosting or supporting GozNym malware. GozNym was responsible for hundreds of thousands of dollars in actual and attempted losses from victims throughout the country, including in the Western District of Pennsylvania. The FBI was able to identify several victims in the Pittsburgh area whose IP addresses were reaching out to the back-end GozNym Avalanche server and had been notified by their financial institutions of suspicious activity on their networks associated with GozNym.

34. On April 11, 2016, the FBI-Pittsburgh Office was notified that Nord-Lock, Inc. (Nord-Lock), a company headquartered in Carnegie, Pennsylvania, had been the victim of an

account take-over (ATO) fraud that resulted in the issuance of a fraudulent wire transfer in the sum of \$378,500 (USD), from PNC Bank in Pittsburgh, Pennsylvania, to D Commerce Bank, AD, account BG83DEMI92401100167438, in Sofia, Bulgaria.

35. According to information provided to the FBI by the Bulgarian General Directorate Combating Organized Crime (hereinafter, "GDBOP"), the above-referenced D Commerce bank account was owned by a business known as Antonio Auto, located at 11 Shumaka Street, Sofia City, Simeonovo, Bulgaria. The owner of Antonio Auto is Martin LAMPIONSKI whose date of birth (DOB) is 03/14/1995. LAMPIONSKI is a Macedonian citizen. The manager of Antonio Auto is Boyan LATINOV. LATINOV's DOB is March 23, 1984, and his phone number is +359889131437.

36. According to GDBOP investigators, LATINOV was listed as the registrant of both email addresses (namely, antonioautol@abv.bg; and antonio.auto@abv.bg) associated with the D Commerce account designated to receive the stolen funds. According to D Commerce Bank login records provided by GDBOP investigators for the time period of February 9, 2016, through April 12, 2016, "Antonio84" was the only user who had logged into the D Commerce bank account. The FBI has reason to believe that LATINOV, who is the manager of Antonio Auto and who was born in 1984, is the user "Antonio 84" and thus was the primary person with access to the D Commerce account for which the stolen Nord-Lock funds were destined.

37. A Nord-Lock employee, hereinafter referred to as H.L., was interviewed by the FBI. According to H.L., on April 07, 2016, a Nord-Lock employee hereinafter referred to as N.B. received an email containing an attachment of a Word document that appeared to be an invoice. Nord-Lock's antivirus logs confirmed that when the attachment was opened by N.B, a malware loader was installed on N.B.'s machine.

38. On April 11, 2016, at approximately 11:00 am, N.B. was having difficulty logging-in to Nord-Lock's PNC Bank (PNC) online banking portal. Around the same time, H.L. became aware that a fraudulent wire transaction for \$378,500 had been initiated from the online account. H.L. immediately notified PNC who initiated a wire recall and notified the FBI in Pittsburgh. Ultimately, the wire transfer was recalled and Nord-Lock suffered no loss.

39. After the fraudulent attempt, H.L. scanned N.B.'s machine with MS Endpoint Virus protection. The antivirus (AV) program quarantined "TojanDownloader:097M." According to the AV logs, this loader was installed on H.B.'s machine on April 7, 2016; the same day H.B. opened the suspicious Word attachment that appeared to be an invoice. Based on my experience and my review of open source materials such as tech industry research reports, I know that this loader, TrojanDownloader:097M, has been used in the recent past to download GozNym malware onto victim machines, which, as described above, was distributed over the Avalanche infrastructure. GozNym malware is a sophisticated malware variant designed to steal online banking credentials. It has been used to target private businesses in the United States since at least January 2016.

40. H.L. consented to the forensic imaging of N.B.'s machine by the FBI. After a forensic analysis of the Nord-Lock machine, GozNym malware was located and identified. No other malware variant was present on the machine.

41. A PNC Bank employee, referred to herein as C.H., was interviewed by the FBI. According to C.H., in addition to the Nord-Lock attempt, PNC had at least two additional fraudulent wire attempts on other PNC corporate banking customers associated with the GozNym Malware. In all three attempts, the referring IP address (i.e., the incoming IP address accessing the PNC accounts) associated with the ATO fraud was 204.155.31.133. As explained

below, this IP address was reported by private industry security researchers as an administrative panel for the GozNym actors. Additionally, multiple banks in the United States that were the victims of GozNym-related ATO fraud advised the FBI that during the attempts the referring IP address was 204.155.31.133.

42. According to information provided by a trusted private industry security expert who has previously provided credible and reliable information to the FBI, IP address 204.155.31.133 was an administrative panel utilized by unknown GozNym actors utilizing the usernames "Craft" and "Salvadordali" to initiate ATO fraud in the United States. The expert advised that Salvadordali typically utilized a VPN service to log-in to the administrative panel, which had the effect of shielding Salvadordali's true IP address. On multiple occasions, however, Salvadordali did not utilize the VPN service and instead logged-in to the administrative panel from the following Bulgarian IP addresses on the following dates and times:

September 4, 2015

IP	Date	Time (EST = GMT -4)
85.91.139.248	2015-09-04	13:11:38
85.91.139.248	2015-09-04	15:13:39
85.91.139.248	2015-09-04	15:13:30
85.91.139.248	2015-09-04	13:05:47
85.91.139.248	2015-09-04	15:17:02
85.91.139.248	2015-09-04	13:10:06
85.91.139.248	2015-09-04	15:18:47
85.91.139.248	2015-09-04	13:08:31
85.91.139.248	2015-09-04	15:15:51
85.91.139.248	2015-09-04	13:14:46
85.91.139.248	2015-09-04	13:07:02
85.91.139.248	2015-09-04	15:20:46
85.91.139.248	2015-09-04	13:05:13
85.91.139.248	2015-09-04	13:13:09
85.91.139.248	2015-09-04	13:05:25

February 15, 2016

IP	Date	Time (EDT = GMT -5)
----	------	---------------------

78.83.25.35	2016-02-15 12:37:21
78.83.25.35	2016-02-15 12:41:57
78.83.25.35	2016-02-15 12:46:27
78.83.25.35	2016-02-15 12:49:09
78.83.25.35	2016-02-15 12:49:35
78.83.25.35	2016-02-15 12:49:41
78.83.25.35	2016-02-15 12:52:57
78.83.25.35	2016-02-15 12:53:53
78.83.25.35	2016-02-15 12:57:02
78.83.25.35	2016-02-15 13:00:30
78.83.25.35	2016-02-15 13:04:02
78.83.25.35	2016-02-15 13:07:51
78.83.25.35	2016-02-15 13:12:16

February 16, 2016

IP	Date	Time (EDT = GMT -5)
78.83.25.35	2016-02-16	02:20:40
78.83.25.35	2016-02-16	02:20:53
78.83.25.35	2016-02-16	02:23:15
78.83.25.35	2016-02-16	02:25:50
78.83.25.35	2016-02-16	03:14:18
78.83.25.35	2016-02-16	03:14:54
78.83.25.35	2016-02-16	03:16:34
78.83.25.35	2016-02-16	03:17:18
78.83.25.35	2016-02-16	03:17:23
78.83.25.35	2016-02-16	03:20:33
78.83.25.35	2016-02-16	03:20:37
78.83.25.35	2016-02-16	03:27:09
78.83.25.35	2016-02-16	03:28:44
78.83.25.35	2016-02-16	03:32:10
78.83.25.35	2016-02-16	03:34:43
78.83.25.35	2016-02-16	03:38:08
78.83.25.35	2016-02-16	03:39:58
78.83.25.35	2016-02-16	03:42:51
78.83.25.35	2016-02-16	03:45:16
78.83.25.35	2016-02-16	03:47:04
78.83.25.35	2016-02-16	03:49:28
78.83.25.35	2016-02-16	03:52:26
78.83.25.35	2016-02-16	03:55:25
78.83.25.35	2016-02-16	03:58:49
78.83.25.35	2016-02-16	04:01:52
78.83.25.35	2016-02-16	04:04:42
78.83.25.35	2016-02-16	04:07:13
78.83.25.35	2016-02-16	04:09:46
78.83.25.35	2016-02-16	04:12:32

78.83.25.35	2016-02-16 04:15:44
78.83.25.35	2016-02-16 04:18:22
78.83.25.35	2016-02-16 04:21:24
78.83.25.35	2016-02-16 04:24:19
78.83.25.35	2016-02-16 04:27:16
78.83.25.35	2016-02-16 04:31:00
78.83.25.35	2016-02-16 04:34:18
78.83.25.35	2016-02-16 04:37:10
78.83.25.35	2016-02-16 04:39:38
78.83.25.35	2016-02-16 04:41:50
78.83.25.35	2016-02-16 04:44:27
78.83.25.35	2016-02-16 04:46:59

March 15, 2016

IP	Date	Time (EST = GMT -4)
78.83.221.66	2016-03-15	19:09:55
78.83.221.66	2016-03-15	19:11:40
78.83.221.66	2016-03-15	19:16:04
78.83.221.66	2016-03-15	19:21:04
78.83.221.66	2016-03-15	19:22:33
78.83.221.66	2016-03-15	19:25:45
78.83.221.66	2016-03-15	19:25:49
78.83.221.66	2016-03-15	19:29:36
78.83.221.66	2016-03-15	19:29:45
78.83.221.66	2016-03-15	19:33:34
78.83.221.66	2016-03-15	19:33:38
78.83.221.66	2016-03-15	19:37:11
78.83.221.66	2016-03-15	19:37:24

March 16, 2016

IP	Date	Time (EST = GMT -4)
78.83.221.66	2016-03-16	03:43:52
78.83.221.66	2016-03-16	03:44:18
78.83.221.66	2016-03-16	03:44:38
78.83.221.66	2016-03-16	03:44:42
78.83.221.66	2016-03-16	03:46:24
78.83.221.66	2016-03-16	03:48:11

May 24, 2016

IP	Date	Time (EST = GMT -4)
78.83.221.66	2016-05-24	10:26:27
78.83.221.66	2016-05-24	10:26:41

June 11, 2016

IP	Date	Time (EST = GMT -4)
78.83.221.66	2016-06-11	03:38:54

June 12, 2016

IP	Date	Time (EST = GMT -4)
78.83.221.66	2016-06-12	02:32:27

43. The FBI conducted a “Whois” look up of the above three IP addresses and found that they resolved to the following:

- a. 85.91.139.248: Mobiltel EAD, 1 Kukush Street, Sofia, Bulgaria, 1309
- b. 78.83.25.35: Mobiltel EAD, 1 Kukush Street, Sofia, Bulgaria, 1309
- c. 78.83.221.66: Mobiltel EAD, 1 Kukush Street, Sofia, Bulgaria, 1309

44. According to information received by the FBI from GDBOP investigators, during the period February 15, 2016, through February 16, 2016, IP address 78.83.25.35 (one of the three aforementioned IP addresses accessing the GozNym malware administrative panel) was assigned to Krasimir NIKOLOV, #7 Ivan Aksakov Street, Entrance A, Apartment 37, Seventh Floor, with a MAC identification number of f8:bf:09:bf:53:5d. A MAC ID (otherwise known as a Media Access Control Address) is a unique identifier assigned to an individual computer by the manufacturer.

45. GDBOP investigators also advised the FBI that during the period from March 15, 2016, through March 16, 2016, IP address 78.83.221.66 (one of the three aforementioned IP addresses accessing the GozNym malware administrative panel) was assigned to Krasimir NIKOLOV, #7 Ivan Aksakov Street, Entrance A, Apartment 37, Seventh Floor, with a MAC ID of f8:bf:09:bf:53:5d.

46. According to GDBOP officials, the following individuals reside at the address of

Ivan Aksakov Street, 7a, Apt. 37, in Varna, Bulgaria:

- d. Krasimir NIKOLOV, DOB May 20, 1972;
- e. Margarita NIKOLOVA (Wife of Krasimir), DOB April 8, 1973; and
- f. Martin (Son of Krasimir) NIKOLOV, DOB August 24, 1997

47. Information regarding IP 85.91.139.248 (one of the three aforementioned IP addresses accessing the GozNym malware administrative panel) was derived from an unrelated investigation conducted by the United States Secret Service. As part of that unrelated investigation, data was pulled from servers hosted at CyberFuel, a hosting company in Costa Rica. On May 24, 2013, pursuant to a Mutual Legal Assistance Treaty (MLAT) request from the United States, the servers were seized and turned over to agents with the U.S. Secret Service. Among the data extracted from the servers was information concerning IP address 85.91.139.248. The data revealed that IP address 85.91.139.248 was utilized to register two money exchanger accounts in early 2013. The registered accounts were as follows:

Username:	Margo100
Email:	autodali69@yahoo.com
Name:	Margarita Nikolova
DOB:	May 20, 1972
Address:	Ivan Aksakov Street, 7a, Apt. 37 Varna, Bulgaria
Phone	+359892355619

Username:	Lansky7297
Email:	krasi2222@gmail.com
Name:	Krasimir Nikolov
DOB:	May 20, 1972
Address:	Varna, Bulgaria
Phone:	+359889505313

48. Based on open source information, the above address (Ivan Aksakov Street, 7a, Apt. 37, Varna, Bulgaria) was listed as the address for KM-Company, Ltd. The Bulgarian phone number +359889505313 was listed as the phone number for KM-Company, Ltd. Based on open

source information, the phone number +359889505313 is associated with advertisements for property and/or hotel rentals in Varna, Bulgaria. The ads were posted by the user Lansky72, and Nikolov was listed as the contact name. The username Lansky72 posted on numerous forums discussing topics such as trojan horse malware and PayPal fraud.

49. From 2013 through 2015, FBI-Pittsburgh was investigating criminal activity on the Darkode criminal forum. In 2014, the username Salvadordali (the same user referenced above seen accessing the GozNym malware administrative panel) was registered on Darkode. The email account autodali69@yahoo.com was provided as Salvadodali's email account. During his time on the Darkode forum, Salvadordali advertised selling fake Bulgarian documents (passports and driver's licenses), selling fake vehicle registrations for multiple European Union countries, and "drops" (i.e., criminals hired to "cash out" funds, often acquired through the commission of cyber-criminal activities, from designated bank accounts) in Bulgaria.


50. The aforementioned facts provide probable cause to believe that Krasimir NIKOLOV and Margarita NIKOLOVA have engaged in violations of Title 18, United States Code, Sections 371 (Conspiracy), 1030(a)(2) (Obtaining Information through an Unauthorized Access of a Protected Computer), 1030(a)(4) (Unauthorized Access of a Protected Computer in Furtherance of Fraud), and 1030(a)(5) (Intentional Damage to a Protected Computer), 1343 (Wire Fraud), 1344 (Bank Fraud), 1349 (Conspiracy to Commit Wire/Bank Fraud) and 1956 (Laundering of Monetary Instruments), (the "Target Offenses"), and that evidence of those crimes, as set forth in Attachment C, will be found in the Target Accounts krasi2222@gmail.com (Attachment A) and autodali69@yahoo.com (Attachment B). Furthermore, based upon the information set forth herein, your affiant has probable cause to believe that the Target Accounts

contain evidence related to the Target Offenses and will yield evidence of the identities of the perpetrators of the offenses.

CONCLUSION

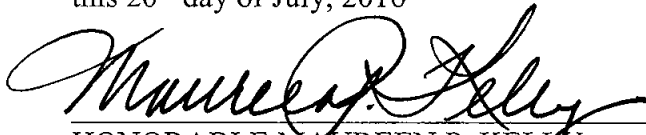
51. Based on the forgoing, I respectfully request that the Court issue the proposed search warrant. Because the warrant will be served on Google and Yahoo who will then compile the requested records at a time convenient to them, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,



Brian Stevens, Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me
this 20th day of July, 2016



HONORABLE MAUREEN P. KELLY
CHIEF UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with email account krasi2222@gmail.com that is stored at premises controlled by Google, a company that accepts service of legal process at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

ATTACHMENT B

Property to Be Searched

This warrant applies to information associated with email accounts autodali69@yahoo.com that are stored at premises controlled by Yahoo, a company that accepts service of legal process at 701 First Avenue, Sunnyvale, CA 94089.

ATTACHMENT C

Particular Things to be Seized

I. Information to be disclosed by Google and Yahoo (the “Provider(s)”)

To the extent that the information described in Attachment A (Google) and/or Attachment B (Yahoo) is within the possession, custody, or control of the Provider, including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, the Provider is required to disclose the following information to the government for the Target Accounts listed in Attachment A (Google) and Attachment B (Yahoo), from inception of the account to the present:

a. The contents of all emails and communications associated with the Target Accounts, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. Content of all information within the Provider’s services enabled and associated with the Target Accounts; such services to include Google Voice, Search History, Google me, Google Drive or Docs, Spreadsheets, Google Profile, Has Plusone, Pp2012, Talk, YouTube, Picasa, Google Services, Google Hangout and any and all other Google services enabled and associated with the Target Accounts.

c. Web history files or documents pertaining to historical searches performed by the user.

d. Files and/or documents pertaining to any Android Devices, Android Market, and Location History.

e. All other communications and messages made or received by the user, including all private messages, chat history, and video calling history.

f. All location information.

g. All IP logs, including all records of the IP addresses that logged into the Target Accounts.

h. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

i. Any accounts associated with the Target Accounts by recovery email, secondary email, SMS recovery number, cookie data; and/or overlapping logins by users with a common IP address;

j. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

k. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

II. Particular Things to be Seized by the Government

All evidence and information described above in Section I that constitutes fruits, contraband, evidence and instrumentalities of the Target Offenses, namely, violations of Title 18, United States Code, Sections 371 (Conspiracy), 1030(a)(2) (Obtaining Information through an Unauthorized Access of a Protected Computer), 1030(a)(4) (Unauthorized Access of a Protected

Computer in Furtherance of Fraud), and 1030(a)(5) (Intentional Damage to a Protected Computer), 1343 (Wire Fraud), 1344 (Bank Fraud), 1349 (Conspiracy to Commit Wire/Bank Fraud) and 1956 (Laundering of Monetary Instruments), from inception of the account to the present, including, for each account or identifier listed on Attachment A and/or Attachment B, information pertaining to the following matters:

1. The content of any and all electronic communication, and any internet search history, other internet activity, or documents, that pertains to:
 - a. The identity of the user(s) of the Target Accounts, to include (but not limited to) names, location of the user, passwords, IP addresses, email communications with other internet accounts (whether email, domain, or any other) under the control of the user(s);
 - b. Evidence pertaining to obtaining unauthorized access to others' computers, particularly through the usage of spear-phishing emails;
 - c. Evidence indicating how and when the email accounts were accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crimes under investigation and to the email account users;
 - d. Evidence indicating the email accounts' user's state of mind as it relates to the crimes under investigation;
 - e. The identity of the person(s) who created or used the accounts, including records that help reveal the whereabouts of such person(s).
 - f. The identity of the person(s) who communicated with the accounts about matters relating to the Target Offenses including records that help reveal their whereabouts;
 - g. Motive for computer intrusion and fraudulent business email compromise activity;
 - h. The illegal trafficking of personal identifying information, usernames and passwords of compromised computers or internet accounts, or any other items which are being offered, requested, or possessed without the authorization of the bona fide owner;
2. Any and all records or other information pertaining to the identity of the subscriber of the Target Accounts, including but not limited to associated email accounts, login IP addresses, and session times and durations.